UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/707,417	11/06/2000	Vance C. Bjorn	003022.P019X	9958

7590 10/02/2006

Judith A. Szepesi
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/707,417	BJORN, VANCE C.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 17 July 2006.

2. Claims 1-31 are pending in the application.

3. Claims 1-31 have been rejected.

Response to Arguments

4. Applicant's arguments, see pages 2 and 3, filed 17 July 2006, with respect to the rejection under 35 U.S.C. 112, first paragraph have been fully considered and are persuasive. The rejection of the claims has been withdrawn. The applicant has shown support in the specification.

5. Applicant's arguments filed 17 July 2006 have been fully considered but they are not persuasive.

On pages 3 and 4, the applicant argues that Hoffman specifically teaches away from a record ID that is "a random number generated for tracking authentication data and disassociating the authentication data from other client identity data".

The examiner respectfully disagrees. Hoffman discloses that the PIN is used for tracking the biometric data in the PIN basket. Hoffman discloses that the buyer selects a PIN of from four to twelve digits from a series of PIN options provided by the system's central database. However, the PIN must be validated by the system. This involves two checks: one, that the number of other buyers using the same PIN aren't too great (since the PIN is used to reduce the number of buyers checked by the biometric comparison algorithm), and that the buyer's registration biometric sample being registered isn't too similar to other buyer's biometrics stored within the same PIN group. If either happens, the enrollment is rejected, an error message is

returned to the BRT, and the buyer is instructed to request a different PIN. The system may optionally return with an "identical match" error condition, which indicates that the buyer already has a record in the system under that PIN. The examiner asserts that the user generates the PIN randomly.

On page 5, the applicant argues that Byford does not teach or suggest the use of a record ID.

The examiner asserts that Hoffman teaches this feature. Byford was not used to teach a record ID.

On page 5, the applicant argues that Towers does not teach or suggest the use of a record ID.

The examiner asserts that Hoffman teaches this feature. Towers was not used to teach a record ID.

On page 5, the applicant argues that Mao does not teach or suggest the use of a record ID.

The examiner asserts that Hoffman teaches this feature. Mao was not used to teach a record ID.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-6, 8, 9, 11-14, 17, 20, 21, 23, 24, 26, 27 and 29-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Hoffman et al U.S. Patent No. 6,594,376 B2.

As to claims 1, 2 and 20, Hoffman et al discloses a method of authenticating a client, the method comprising:

receiving a record ID for a user, the record ID being a random number generated for tracking authentication data and disassociating the authentication data from other client identity data, and a one-time key generated by a third party server and encrypted with a user's public key by the server [column 12, lines 1-45];

receiving the user's authentication data from the client [column 12, lines 46-62];

determining if the user's authentication data matches the record ID [column 14, lines 57-61]; and

if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client [column 36, lines 10-40].

As to claims 2 and 20, Hoffman et al discloses the method further comprising registering the user with the authentication server, registering comprising:

receiving a registration authentication data from the user [column 33, lines 26-42];

generating a random public key/private key pair for the user [column 33, lines 26-42];

generating the random number as the record ID for the user [column 33, lines 26-42]; and

associating the authentication data and the private key with the record ID [column 33, lines 26-42].

As to claims 3 and 21, Hoffman et al discloses sending the record ID and the public key to the user [column 31, lines 55-59].

As to claim 4, Hoffman et al discloses establishing a secure connection with the user, prior to receiving registration authentication data [column 32, lines 1-7].

As to claims 5 and 23, Hoffman et al discloses a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server [column 32 line 64 to column 33 line 12].

As to claims 6 and 24, Hoffman et al discloses that the client's authentication data is automatically redirected to the authentication server [column 32 line 64 to column 33 line 12].

As to claims 8 and 26, Hoffman et al discloses that the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card [column 32 line 64 to column 33 line 12].

As to claims 9 and 27, Hoffman et al discloses that the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key [column 33, lines 26-42].

As to claims 11 and 29, Hoffman et al discloses that the record ID and the encrypted one-tune key are further encrypted using a partner key. Hoffman et al discloses decrypting the record ID and encrypted one-time key using the partner key [column 33, lines 26-42].

As to claims 12 and 30, Hoffman et al discloses that the partner key is a symmetric key set up during registration of the partner [column 33, lines 26-42].

As to claims 13 and 31, Hoffman et al discloses that the partner key is a private key of the authentication server [column 33, lines 26-42].

As to claim 14, Hoffman et al discloses a method of using an authentication server to authenticate a user to a third party server, the method comprising the third party server:

> looking up a record ID associated with the user, the record ID being a random number generated to track the user's authentication data and used to separate the user's other identity information from the authentication data [column 12, lines 1-45];
>
> generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user [column 12, lines 46-62];
>
> receiving the authentication data, the authentication data being the decrypted one-time key decrypted with the user's private key by the

authentication server, such that the user does not have control of the user's private key at any time [column 14, lines 57-61]; and

permitting access to the server [column 14, lines 57-61].

As to claim 17, Hoffman et al discloses a third-party authentication system comprising:

an authentication server to receive a record ID for a user, the record ID being a randomly generated number used to separate the user's other identity information from the user's authentication data, and a one-time key generated by a third party server and encrypted with a user's public key by the third party server, as discussed above;

a comparison logic in the authentication server to receive the user authentication data from the client and determine whether the user's authentication data matches the record ID, as discussed above; and

a decryption logic in the authentication server to decrypt the one-time key with a private key associated with the validated record ID, and to return the decrypted one-time key to the client, as discussed above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 7, 10, 25 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al U.S. Patent No. 6,594,376 B2 as applied to claim 1 above, and further in view of Byford U.S. Patent No. 6,581,161 B1.

As to claims 7, 10, 25 and 18, Hoffman et al teaches that the authentication data is biometric data [Hoffman et al figure 1].

Hoffman et al does not teach discarding the record ID after returning the one-time key to the user.

Byford teaches authentication data being biometric data [column 4 lines 44-58]. Byford teaches discarding a user's record ID [column 2, lines 39-42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al so that the authentication data was biometric data and the user's record ID would have been discarded.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al by the teaching of Byford because it removes the need for encoded badges, static passwords and the like, and also removes the need for users to present themselves at a particular location, such as a security control office, before they can be granted access rights to a facility [column 4, lines 59-67].

8. Claims 15, 16, 18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al U.S. Patent No. 6,594,376 B2 as applied to claims 14 and 17 above, and further in view of Towers et al U.S. Patent No. 5,692,106.

As to claims 15, 16 and 18, Hoffman et al does not teach determining an authentication policy associated with the user. Hoffman et al does not teach verifying that the authentication policy has been satisfied, prior to permitting access to the server. Hoffman et al does not teach determining if the server should verify additional data. Hoffman et al does not teach requesting additional data from the user prior to generating the onetime key.

Towers et al teaches determining an authentication policy associated with the user [column 13, lines 31-48]. Towers et al teaches verifying that the authentication policy has been satisfied, prior to permitting access to the server [column 13, lines 31-48]. Towers et al teaches determining if the server should verify additional data [column 1, lines 36-63]. Towers et al teaches requesting additional data from the user prior to generating the one-time key [column 1, lines 36-63].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al so that an authentication policy associated with the user was verified prior to permitting access to the server. Should additional user information was needed; it would have been requested prior to generating the one-time key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al by the teaching of Towers et al because the examiner asserts that authentication policies restrict what a user can do on a server site and requesting additional data further authenticates a user prior to accessing a server's site.

As to claim 21, Hoffman et al teaches that the interface sends the record ID and the public key to the user, as discussed above.

9. Claims 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al U.S. Patent No. 6,594,376 B2 as applied to claim 17 above, and further in view of Mao U.S. Patent No. 6,119,227.

As to claim 19, Hoffman et al does not teach nonce generation logic to generate a nonce. Hoffman et al does not teach that the nonce is to be included with the user authentication data from the client. Hoffman et al does not teach comparison logic to verify that the user authentication data includes the appropriate nonce.

Mao teaches nonce generation logic to generate a nonce [column 5, lines 13-29]. Mao teaches that that the nonce is to be included with the user authentication data from the client [column 5, lines 30-51]. Mao teaches comparison logic to verify that the user authentication data includes the appropriate nonce [column 5, lines 30-51].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al so that there was nonce generation logic to generate a nonce. The nonce is would have been included with the user authentication data from the client. Comparison logic would have been used to verify that the user authentication data includes the appropriate nonce.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Hoffman et al by the teaching of Mao because it provides a method for authenticating a user's requests and messages [column 1, lines 49-67]

As to claim 22, Hoffman et al teaches that interface establish a secure connection with the user, prior to receiving registration authentication data, as discussed above.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AKM
September 25, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

CR 9/27/06